IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for tracking a virus comprising:

copying from a first packet received at a destination host to which the first packet is addressed an information including a sender information usable to determine a sending source that addressed and sent the first packet to the destination host, wherein the information is copied from the first packet based at least in part on a determination that the first packet comprises an open packet;

passing through a second packet associated with the first packet, without copying from the second packet said information including a sender information, based at least in part on a determination that the second packet does not comprise an open packet;

saving the ~~copied~~ information copied from the first packet;

determining whether an infection has been received, wherein the infection is associated with a network transmission with which the first and second packets are associated;

retrieving the saved information; and

using the saved information to identify and take a responsive action with respect to the sending source.

2. (Original) The method of claim 1, wherein the information includes a file system location.

3. (Original) The method of claim 1, wherein the information includes a file name.

4. (Original) The method of claim 1, wherein the information includes a network address of a source computer.

5. (Previously Presented) The method of claim 1, wherein the information is saved on the destination host.

6. (Original) The method of claim 1, wherein the determination of when a virus has been received is performed when an attempt to write a file occurs.

7. (Original) The method of claim 1, wherein the determination of when a virus has been

received is performed when an attempt to open a file occurs.

8. (Original) The method of claim 1, wherein the determination of when a virus has been received is performed when an attempt to read a file occurs.

9. (Original) The method of claim 1, wherein the determination of when a virus has been received is performed when an attempt to create a file occurs.

10. (Original) The method of claim 1, wherein the determination of when a virus has been received is performed when an attempt to delete a file occurs.

11. (Original) The method of claim 1, wherein the determination of when a virus has been received is performed when an attempt to access a file occurs.

12. (Canceled)

13. (Previously Presented) The method of claim 1, wherein the network transmission includes a plurality of network packets.

14. (Original) The method of claim 1, further comprising copying information from a third packet and saving the copied information.

15. (Original) The method of claim 1, further comprising copying and saving information from a plurality of packets, wherein the plurality of packets are a subset of a network transmission.

16. (Original) The method of claim 15, further comprising passing through a second plurality of packets, wherein the second plurality of packets are a second subset of the network transmission.

17. (Original) The method of claim 1, wherein information includes a username.

18. (Original) The method of claim 1, wherein information includes a user credential.

19. (Original) The method of claim 1, wherein information includes a name of a source computer.

20. (Original) The method of claim 1, wherein information includes a netbios name.

21. (Original) The method of claim 1, wherein information includes a domain name service name.

22. (Currently Amended) A system for tracking a virus comprising:

a processor configured to copy from a first packet received at a destination host to which the first packet is addressed an information including a sender information usable to determine a sending source that addressed and sent the first packet to the destination host, wherein the information is copied from the first packet based at least in part on a determination

that the first packet comprises an open packet; pass through a second packet associated with the first packet, without copying from the second packet said information including a sender information, based at least in part on a determination that the second packet does not comprise an open packet; save the ~~copied~~ information copied from the first packet; determine whether an infection has been received, wherein the infection is associated with a network transmission with which the first and second packets are associated retrieve the saved information ; and use the saved information to identify and take a responsive action with respect to the sending source; and

a memory coupled with the processor, wherein the memory is configured to provide the processor with instructions.

23. (Currently Amended) A computer program product for tracking a virus, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

copying from a first packet received at a destination host to which the first packet is addressed an information including a sender information usable to determine a sending source that addressed and sent the first packet to the destination host, wherein the information is copied from the first packet based at least in part on a determination that the first packet comprises an open packet;

passing through a second packet associated with the first packet, without copying from the second packet said information including a sender information, based at least in part on a determination that the second packet does not comprise an open packet;

saving the ~~copied~~ information copied from the first packet;

determining whether an infection has been received, wherein the infection is associated with a network transmission with which the first and second packets are associated

retrieving the saved information; and

using the saved information to identify and take a responsive action with respect to the sending source.